## REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claims 1-3, 5, 9, 16-22 have been amended. Claims 1-11 and 13-22 are pending in this application. The amendments to the claims do not add any new matter. Furthermore, the amendments to the claims were made to correct typographical errors and to improve readability of the claims, and not for any reason related to patentability. No new claims are added or cancelled. Each pending claim is in condition for allowance over the cited art because one or more elements of each pending claim is not disclosed, taught, or suggested by the cited art.

All issues raised in the Final Office Action mailed November 3, 2004 are addressed hereinafter.

## REJECTION OF CLAIMS 1 and 16-18 UNDER 35 U.S.C. § 112

Claims 1 and 16-18 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Claims 1 and 16-18 have been amendment in this paper to address the 35 U.S.C. 112, second paragraph, issue. Applicants therefore respectfully request withdrawal of the rejection under 35 U.S.C. § 112, second paragraph.

## REJECTION OF THE CLAIMS UNDER 35 U.S.C. § 103(a)

Claims 1-4, 9-11 and 13-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *An,* U.S. Patent No. 6,031,904. Claims 5-8 and 19-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *An,* in view of *Sladek,* U.S. Patent No. 6,622,016. The rejections are herein respectfully traversed.

*An does not teach an Authorization Service separate from an Authentication Server*

Independent Claim 9, representative of independent claims 1, 16, 17, 18, recites:

- authenticating the subscriber by an authentication server;
- generating a privilege token associated with the subscriber by an authorization service, *said authorization service separate from said authentication server*;

*An* does not teach or suggest each and every element of these limitations.

As is described in the Background section of the current specification, prior service subscription management systems suffer from a "lack of an authorization model. Any user can subscribe to any service. In order to provide differentiated services, an authorization model is essential." (Page 2, lines 16-17.) As in *An*, any user can subscriber to any service. The claimed invention solves this problem by separating service management and selection from user authentication processing. (Page 4, lines 22-23, Page 8, line 11.)

As is clearly shown in Fig. 1, Authentication Server 106 is separate from Authentication Service 114. As described at Page 11, line 21, the authentication server is used primarily for user authentication. As described at Page 10, lines 24-26, authorization service 114 provides security and client authorization functions, including determining which privileges are associated with a user.

Claims 1, 9, and 16-18, as amended, all feature that the authorization process is separate from the authentication server.

The Office Action asserts on Page 10, third paragraph, that "as a term of art, authentication and authorization are used nearly if not always interchangeably." Applicants respectfully disagree. According to "www.whatis.com", a website frequently used by those

skilled in the art, "authentication" is defined as "a process of determining whether someone or something is, in fact, who or what it is declared to be." "Authorization" is defined as "the process of giving someone permission to do or have something." Further, the website states that "[l]ogically, authorization is preceded by authentication."

The different nature of authentication and authorization functions is also recognized in IETF RFC 2903 and RFC 3539.

As is known by those skilled in the art, a user may be authenticated yet not have authorization to perform all tasks. For example, an administrator user typically has greater permissions than most other users. An authorization process determines whether a given user has the authority to issue a particular command. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Once a user has been authenticated, then he may be authorized for different types of access or activity.

*An* teaches that "the server performs subscriber authentication by requesting the DN and PIN." (Col. 5, lns 12-13). *An* only teaches authentication, and does not teach or suggest any type of authorization service, much less an authorization service separate from the authentication server.

Accordingly, it is respectfully submitted that independent Claims 1, 9, 16, 17 and 18 are patentable over the cited art and are in condition for allowance. Claims 2-4 and 10-11 are dependent claims, each of which depends (directly or indirectly) on one of the independent claims, and are therefore allowable for the reasons given above for the claim on which it depends.

*An does not teach Privilege Tokens*

Independent Claim 1, representative of independent Claims 5, 16, 17, 18 recites:

- determining, based on privilege information in the privilege token associated with the subscriber generated by the authorization service, whether the subscriber has privileges sufficient to carry out the requested modification;

Independent Claim 9 similarly recites:

- determining whether the subscriber is allowed to automatically log into the telecommunications services, said determination based on privilege information in the privilege token associated with the subscriber;

*An* does not teach or suggest determining whether a subscriber has privileges

sufficient to carry out a modification, or automatically log into telecommunications services,

based on privilege information in a privilege token.

With respect to privilege tokens, the Office Action states at Page 4:

What An et al. does not teach is the use of a privilege token, but tokens are very old and well known in the art as merely one means of effecting validation. A token can be any piece/bit of information/data used to compare data such as the aforementioned directory number and PIN with... It would have been obvious for one of ordinary skill in the art to use a privilege token method of validation inasmuch as again, it is merely one of a plurality of well known methods of validation.

The Office Action further states at Page 10:

As to the applicant's argument regarding the privilege token, again examiner maintains that the use of privilege tokens are obvious. Privilege tokens are a known method of authentication. The suggestion in An et al. that examiner relies on is the fact that An et al. implements an authentication procedure.

The Office Action appears to rely on inherency without admitting so. This reliance is

misplaced. There is no suggestion in the references to adapt a token data structure in the

manner claimed by the Applicants.

As discussed above, authentication and authorization are separate processes. In the claims, once a subscriber is authenticated, a privilege token is generated by the authorization service. This privilege token is used to provide differentiated services.

Privilege information in the privilege token associated with the subscriber is used to determine whether the subscriber has privileges sufficient to carry out the requested modification (Claims 1, 5, 16, 17, 18) or to automatically log in to subscribed services (Claim 9). The Examiner merely focuses on the known general use of tokens in the rejection of these claims. The claims, however, recite a <u>privilege</u> token that includes privilege information. Nothing in the cited references teaches or suggests a <u>privilege</u> token.

Furthermore, the Examiner cites the specific example of using a token to effect authentication. A <u>privilege</u> token as used in the claims is not used to effect authentication. Rather, it is used to provide differentiated services to users who have already been authenticated.

With respect to claims 1, 5, and 16-18, the privilege token is used to determine if a subscriber has privileges sufficient to modify his subscription. Representative Claim 1 recites:

> if the subscriber is determined to have sufficient privileges, the method further
> comprising the steps of:

before the receiving, modifying, sending and generating steps. Only if a subscriber is both authenticated *and authorized to access a particular service* (i.e. has sufficient privileges) is the subscriber allowed to modify his subscription.

The use of the privilege token enables the subscription management service to provide differentiated services to subscribers. Even if the cited references taught use of a

-20-

token to effect authentication, which they do not, using a token to implement authentication

is quite different from determining whether a subscriber has privileges sufficient to modify

his subscription based on privilege information in a privilege token.

In addition, with respect to Claim 9, the privilege token is used to determine whether

a subscriber can automatically log into subscribed services. The Office Action asserts that

Col. 5, lines 35-48 of *An* teaches that "the subscriber is actually 'logged in' as they are able

to amend each feature on their current profile." (Office Action, Page 7). However, claim 9

recites:

> - if the subscriber is allowed to automatically log into the telecommunications
> services, receiving, from the directory repository, a list of all services for which the
> subscriber is then currently subscribed; and automatically logging the subscriber into
> all services identified in the list.

The cited section of *An* only teaches that subscribers can "access and amend their

feature profiles." The subscriber is only logged into the service provider's feature profile

system, not the feature profiles themselves. The system of *An* provides a list of feature

profiles for the subscriber. The subscriber can only amend profiles; he never *logs into the*

*feature profiles.* Claim 9 recites: "automatically logging the subscriber into all services

identified in the list." The cited references do not teach or suggest this limitation.

Accordingly, it is respectfully submitted that independent Claims 1, 5, 9, 16, 17 and

18 are patentable over the cited art and are in condition for allowance. Claims 2-4, 6-8 and

10-11 are dependent claims, each of which depends (directly or indirectly) on one of the

independent claims, and are therefore allowable for the reasons given above for the claim on

which it depends.

*An does not teach determining privileges based on roles*

Dependent Claim 2 recites:

creating and storing in the privilege token *one or more roles occupied by the subscriber* based on role information that is stored in the directory repository, *said stored role information including mapping information that maps a role to one or more privileges that specify which telecommunications services a subscriber having that role can subscribe to*

Independent Claim 19, representative of independent Claims 20-22, recites:

generating a list of the one or more services to which the subscriber is currently subscribed, based on group membership of the subscriber, *one or more roles occupied by the subscriber*, and authorization information associated with the subscriber that is stored in the directory repository, *wherein said one or more roles are mapped to one or more privileges that specify which telecommunications services a subscriber having that role can subscribe to*

The Office Action asserts that "a subscriber in An et al. may have more than one line, i.e., a landline, a wireless subscription, pager service, local and/or long distance service, etc. read as the claimed roles." (Office Action, Page 7). As required by Claims 2 and 19-22, a role is *mapped to one or more privileges* that specify which telecommunications services a subscriber can subscribe to. By reading the role information from a privilege token, the claimed invention can determine the subscriber's privileges by looking up the privileges mapped to the subscriber's role. "Roles" as recited in the present invention do not read on multiple telephone lines, as telephone lines are not associated or mapped to any privileges. The cited references do not teach or suggest Claims 2 and 19-22.

Accordingly, it is respectfully submitted that independent Claims 19-22 and dependent Claim 2 are patentable over the cited art and are in condition for allowance for at least these reasons.

*Storing privilege information in a directory repository is not taught by the cited references*

The Office Action combines Claims 1 and 13 in the rejection under 35 U.S.C. §

103(a). However, the limitations of Claim 1 and Claim 13 are quite different. Independent

Claim recites:

- receiving a request from the subscriber to obtain a list of available
  telecommunications services;
- generating a list of only those telecommunications services for which the subscriber
  has a privilege to subscribe to, based on privilege information and service
  information that is stored in the directory repository and associated with the
  subscriber, said privilege information associated with the subscriber
  specifying what telecommunications services the subscriber has privileges to
  subscribe to;
- receiving a subscriber selection of one of the telecommunications services from the
  generated list of telecommunications services

With respect to Claim 13, the Office Action asserts that "feature profiles are stored

locally either on server 50, machine 52, as well as in profile repository 18", and that profile

changes to a profile are sent to the profile repository 18. (Office Action, Page 3).

Use of a profile repository does not teach or suggest storing privilege information and

service information in a directory repository, as featured by Claim 13. *An* does not teach or

suggest any type of privilege information, much less storing privilege information in a

directory repository. Furthermore, Claim 13 requires "generating a list of only those

telecommunications services for which the subscriber has a privilege to subscribe to." *An*

does not provide any type of differentiated services, as all users in *An* can access all feature

profiles, and therefore cannot teach or suggest generating a list of only those services for

which a subscriber has a privilege to subscribe to.

Accordingly, it is respectfully submitted that independent Claim 13 is patentable over

the cited art and are in condition for allowance. Dependent Claims 14-15 are dependent

claims, each of which depends (directly or indirectly) on one of the independent claims, and are therefore allowable for the reasons given above for the claim on which it depends.

## Conclusion

In addition to the above-discussed limitations, each of the dependent claims introduces one or more additional limitations that independently render it patentable. However, in view of the patentability of the independent claims, the dependent claims are not further argued at this time to expedite prosecution.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is invited to contact the undersigned by telephone if the Examiner believes that such contact would be helpful in furthering the prosecution of this application. If there are any additional charges, please charge them to Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Lesley Coulson Boveri
Reg. No. 46,642
Date: February 2, 2005

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
(408) 414-1210
Facsimile: (408) 414-1076

| CERTIFICATE OF MAILING |
| --- |
| I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450. |
| on _February 2, 2005_ by |

-24-